Puissances de 2 et de 3

Christian Aebi, Collège Calvin, Geneva, Switzerland 1211, christian.aebi@edu.ge.ch

Préambule. *L'origine du texte ci-dessous est une lettre remise à Jacques Fleury, directeur du Collège Calvin de 1986 à 2009, lors de son départ à la retraite [1].*

Petit jeu de calcul

Problème 1. *Peut-on écrire tout nombre premier sous la forme d'une somme ou d'une différence de deux termes, chacun étant une puissance de 2 ou de 3 ?*

Pour entrer en matière, il n'est pas inutile d'énumérer quelques puissances de 2 et de 3 :

$2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$, $2^6 = 64$, $2^7 = 128$ et
$3^0 = 1$, $3^1 = 3$, $3^2 = 9$, $3^3 = 27$, $3^4 = 81$, $3^5 = 243$ et $3^6 = 729$.

Combinons ces puissances en effectuant des sommes ou des différences de deux termes, afin de générer le plus de premiers consécutifs possibles :

$$\begin{aligned}
2 &= 2^0 + 3^0 \quad , & 3 &= 2 + 3^0 \quad , & 5 &= 2 + 3 \quad , \\
7 &= 3^2 - 2 \quad , & 11 &= 2^3 + 3 \quad , & 13 &= 2^2 + 3^2 \quad , \\
17 &= 2^3 + 3^2 \quad , & 19 &= 3^3 - 2^3 \quad , & 23 &= 2^5 - 3^2 \quad , \\
29 &= 2 + 3^3 \quad , & 31 &= 2^2 + 3^3 \quad , & 37 &= 2^6 - 3^3 \quad , \\
41 &= 2^5 + 3^2 \quad , & 43 &= 2^4 + 3^3 \quad , & 47 &= 2^7 - 3^4 \quad .
\end{aligned}$$

Remarque. L'unicité de l'écriture n'est pas garantie, puisque l'on a aussi que $19 = 2^4 + 3$.

Et 53 alors ?

Problème 2. *Comment passer d'une équation 'exponentielle' à une courbe elliptique ?*

Le fait que 53 ne puisse s'écrire sous la forme d'une *somme* de deux termes dont l'un est une puissance de 2 et l'autre de 3 se vérifie facilement en effectuant les $6 \cdot 4$ combinaisons possibles des sommes de ces derniers, chacun d'entre eux étant strictement plus petit que 53. D'une manière similaire, 4^2 calculs permettent de s'assurer que $|3^n - 2^m| \neq 53$, quels que soient les nombres naturels n et m inférieurs à 4. Pour la suite, on suppose donc que m et n sont plus grands ou égaux à 4.

La clef de la solution, concernant $|3^n - 2^m|$ réside dans une utilisation judicieuse du calcul modulo un nombre bien choisi. Tout d'abord, prouvons que l'équation $3^n - 2^m = 53$ n'admet aucune solution entière. En effet, il suffit de la regarder dans $\mathbb{Z}_8$ pour qu'elle devienne $3^n \equiv 5 \pmod 8$. Or, cette congruence est absurde, puisque si n est pair on a $1 \equiv 5 \pmod 8$ et si n est impair, on a $3 \equiv 5 \pmod 8$.

Ensuite, montrons que l'équation $2^m - 3^n = 53$ n'admet aucune solution entière. Comme $m > 3$ alors en la regardant dans $\mathbb{Z}_{16}$, on obtient $-3^n \equiv 5 \pmod{16}$. Or, les puissances de 3 dans $\mathbb{Z}_{16}$ sont $3 \to -7 \to -5 \to 1$, d'où $n = 4 \cdot k + 3$. D'autre part, si l'on observe notre équation dans $\mathbb{Z}_{27}$, on obtient $2^m \equiv -1 \pmod{27}$. D'où, en considérant les puissances de 2 dans $\mathbb{Z}_{27}$, $2 \to 4 \to 8 \to -11 \to 5 \to 10 \to -7 \to 13 \to -1$, l'on déduit que $m = 18 \cdot l + 9$. Substituons, puis récrivons l'équation sous la forme : $53 = 2^{3\cdot(6l+3)} - 3^{4k+3} = \left(2^{6l+3}\right)^3 - 27 \cdot \left(3^{2k}\right)^2$. Posons $x := 2^{6l+3}$ et $y := 3^{2k}$ pour obtenir finalement la *courbe elliptique* $x^3 - 27y^2 = 53$.

Un aller-retour !

Problème 3. *Quel regard porter sur $x^3 - 27y^2 = 53$ pour conclure ?*

De prime abord, on pourrait imaginer devoir utiliser l'artillerie de la théorie des courbes elliptiques. Or, une petite astuce, qui m'a tout de même demandé sept jours de cogitation active et passive, permet de porter l'estocade finale au problème. Il suffit de regarder $x^3 - 27y^2 = 53$ dans $\mathbb{Z}_7$ et oh ! surprise, l'équation devient $x^3 + y^2 \equiv 4 \pmod{7}$. Or,

1. les seuls cubes dans $\mathbb{Z}_7$ sont 0, 1 et 6 et
2. les seuls carrés sont 0, 1, 2 et 4.

Par conséquent, on aurait $x \equiv 0 \pmod{7}$, alors que $x = 2^{6l+3}$. □

Postscriptum

Le problème traité ci-dessus de manière élémentaire est conjecturé dans l'ouvrage [2]. Sa preuve pourrait être contenue sur une demi-page A4. Sous cette dernière forme elle devrait paraître à l'avenir dans l'American Mathematical Monthly. L'intérêt de cette note est davantage de présenter une narration de recherche et de tenter de sensibiliser un littéraire, J. Fleury, au monde fascinant de l'arithmétique. Une question qui me turlupine encore et que je soumets à mes chers lecteurs est de prouver qu'il existe une infinité de nombres premiers ne pouvant pas s'écrire sous la forme $|2^n \pm 3^m|$.

Références

[1] URL : http ://icp.ge.ch/po/calvin/espace-pedagogique/math/cours-de-c.-aebi/J_Fleury.pdf/

[2] Chris K. Caldwell, G. L. Honaker, Jr *Prime Curios ! The Dictionary of Prime Number Trivia*, Reference / Trivia, Nov 04 2009, Cf. https ://primes.utm.edu/curios/